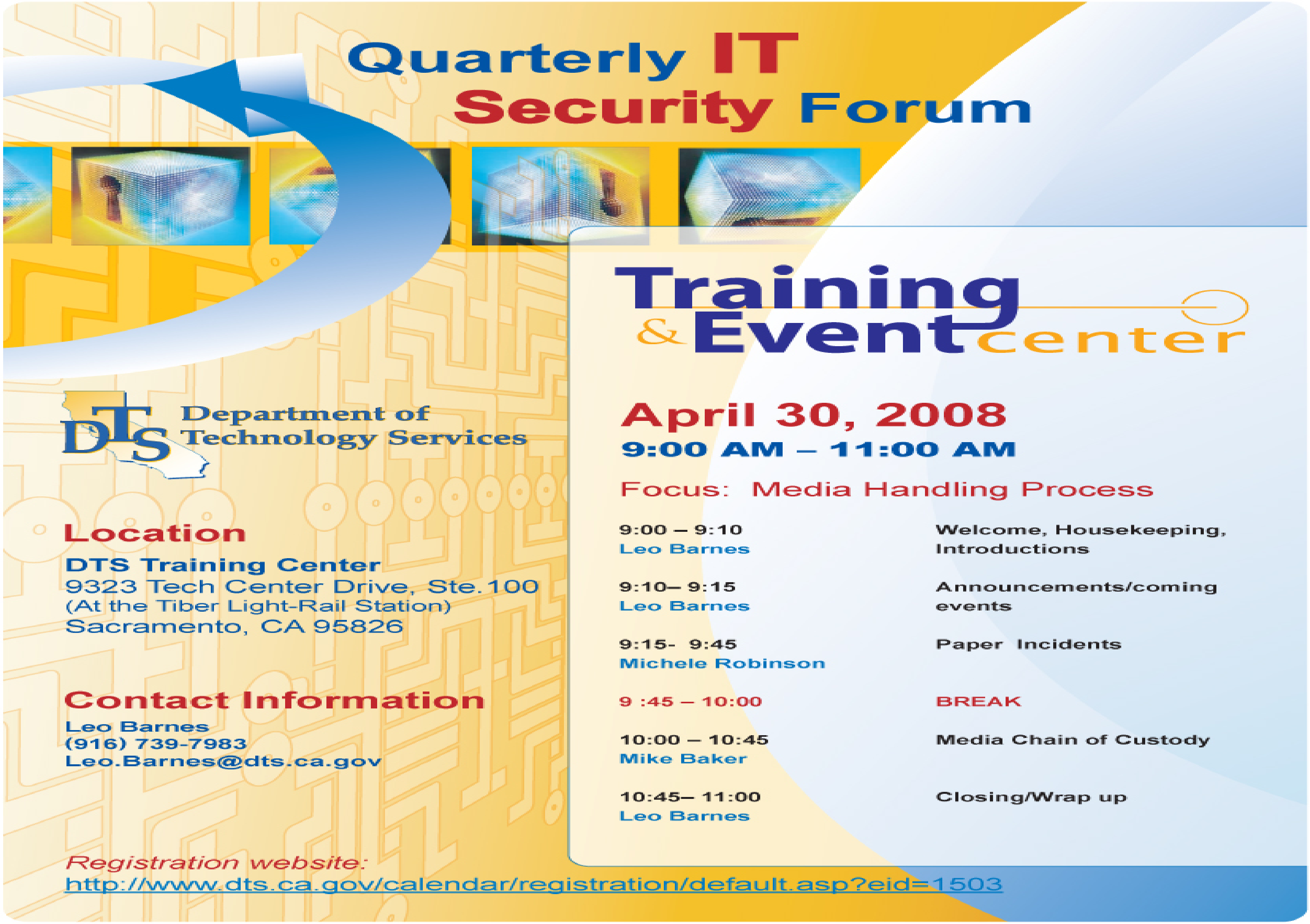


Quarterly IT Security Forum

Department of Technology Services

Training & Event center

April 30, 2008

9:00 AM – 11:00 AM

Focus: Media Handling Process

9:00 – 9:10 Leo Barnes	Welcome, Housekeeping, Introductions
9:10– 9:15 Leo Barnes	Announcements/coming events
9:15- 9:45 Michele Robinson	Paper Incidents
9 :45 – 10:00	BREAK
10:00 – 10:45 Mike Baker	Media Chain of Custody
10:45– 11:00 Leo Barnes	Closing/Wrap up

Location

DTS Training Center
9323 Tech Center Drive, Ste. 100
(At the Tiber Light-Rail Station)
Sacramento, CA 95826

Contact Information

Leo Barnes
(916) 739-7983
Leo.Barnes@dts.ca.gov

Registration website:
http://www.dts.ca.gov/calendar/registration/default.asp?eid=1503

Welcome

- **Welcome!**
  - **Leo Barnes**
    DTS Security Awareness Coordinator
  - **Presentation Slides will be available on the DTS website soon.**
  - **Please complete your Evaluation Surveys!**

Upcoming DTS Events

- **Customer Forum: DTS Annual Report to Customers at GTC**
  - **May 14**
- **DTS - Gartner Technology Day: Shared Services**
  - **June 3**
- **DTS - Gartner Technology Day: ITIL Next Steps**
  - **September 28**
- **Link to DTS Event Calendar: http://www.dts.ca.gov/calendar/default.asp**

CALIFORNIA OFFICE OF
INFORMATION SECURITY
& PRIVACY PROTECTION

Paper Incidents: Their Impact and Mitigation Strategies

Presented by

Michele Robinson

April 30, 2008

Topics

- Data breach
- Type and frequency of breaches involving paper
- Affect of breaches
- Primary causes
- Recommended practices and mitigation strategies (policy, process, and human)

Data Breach

- Compromise of personal information
- California defines personal information:
  - Broadly in Civil Code Section 1798.3
  - Narrowly in Civil Code Section 1798.29
- Various Mediums
  - Paper
  - Electronic
  - Verbal

Types of Data, Size and Frequency

- Not just Personal Information
  - Network diagrams
  - Building plans
  - Other documents classified by the organization as confidential or sensitive
- S to XXXL in size
- One time to recurring daily, weekly, monthly

Affect of Breaches

- Individual victims
- Monetary loss
- Productivity loss
- Embarrassment
- Terminations
- Loss of public trust!

Primary Causes

"There is no need to sally forth, for it remains true that those things which make us human are, curiously enough, always close at hand. Resolve, then, that on this very ground, with small flags waving and tiny blasts of tiny trumpets, **we shall meet the enemy, and not only may he be ours, he may be us."**

- *Pogo (as depicted by Walt Kelly)*

Primary Causes

- Handling/processing errors
- Lack of sufficient internal controls
- Carelessness/negligence
- Policy violations
- Criminal activity (insider threat)
- Lost in the mail
- Criminal activity (outsider threat)

Mitigation Strategies General Rule

- Back to basics
- Security and internal controls:
  - Administrative
  - Technical
  - Physical
- With paper –administrative and physical controls are more pervasive

Mitigation Strategies
Policy Focus

- Must have policy
  - Principle mission/purpose
  - Sets management expectations
  - Consequence of errors and non-compliance
- Helps everyone understand
  - What their role and purpose is
  - What happens or could happen when/if error or

    or non-compliance occurs

Mitigation Strategies
Process Focus

- Review manual business processes
- Understand the purpose and why it is or has been done that way
- Learn about any other methods attempted and why this did or did not work
- Review all paper documents and forms used to collect information and support business processes…particularly those that contain personal information

Mitigation Strategies Process Focus *(cont.)*

- Eliminate use of the personal information from both where possible
- The best rule to apply here: Where it absolutely is NOT necessary and has no purpose—eliminate its use!
- Retire old processes and forms

Mitigation Strategies Process Focus *(cont.)*

- Document processes/procedures
- Update and maintain documentation as changes occur
- Procedure manuals (how-to for staff)
- Identify the root cause of problem(s) with current processes
- Treat the problem not just the symptom(s)

Mitigation Strategies
Human Focus

- □ Awareness - Train, train, train!
- □ Accountability
  - Work schedules, assignments and rotation support knowledge of who did what and when
  - Clearly defined roles & responsibilities
  - Employee sign-off or initial on various steps in the work-flow process
  - Quality assurance and/or peer reviews

Mitigation Strategies Human Focus *(cont.)*

- Accountability
  - Signed acknowledgement forms
  - Performance reviews
  - Remedial and refresher training
  - Appropriate discipline/sanctions for policy violations
- These are continuous ongoing management functions which can not be left unattended

Mitigation Strategies
Case Study – One Example

Symptoms of Internal Control Deficiencies

- Complaints/reports of privacy violations
  - Documents discovered unattended
  - Documents reported being left in plain view
- Missing files
- Lost mail packages
- Other factors

Mitigation Strategies
Case Study - Example

- Executive Management directive and procedures issued in response
- Reinforced:
  - at staff meetings
  - through update to staff procedure manuals
  - Through remedial training where necessary

Additional Resources

- □ AIIM – ECM Association at www.aiim.org

  A resource for information, strategies, tools, and articles like the one at http://www.aiim.org/article-aiim.asp?ID=31456 entitled “Don’t Forget the Paper”

- □ Association of Records Managers and Administrators now known as ARMA-International at www.arma.org

  A resource for standards, strategies, guidance, and tools on records management and security like the Risk Profiler Self-Assessment for Records and Information Management tool found at http://www.arma.org/standards/index.cfm

Questions

Department of Technology Services

Media Chain of Custody

Where We Are

- Security breaches are a state-wide problem.
- Disclosure laws are making it more costly for security breaches.
- In 2006, the State averaged four security incidents per week.
- Security breaches resulted in extensive discovery efforts and had the potential for the loss of customer confidence.
- Security breaches led to DTS implementing the Chain of Custody system and eventually hiring a consultant to look at processes.

The Washington Post

AN INDEPENDENT NEWSPAPER

Two Navy recruiters laptops stolen...

The Mercury News

MercuryNews.com

Kaiser laptop stolen; patient addresses on it

The New York Times

Two teenagers were arrested Saturday in the theft of a laptop and hard drive containing secret data on up to 26.5 million veterans and military personnel, the authorities said.

By THE ASSOCIATED PRESS

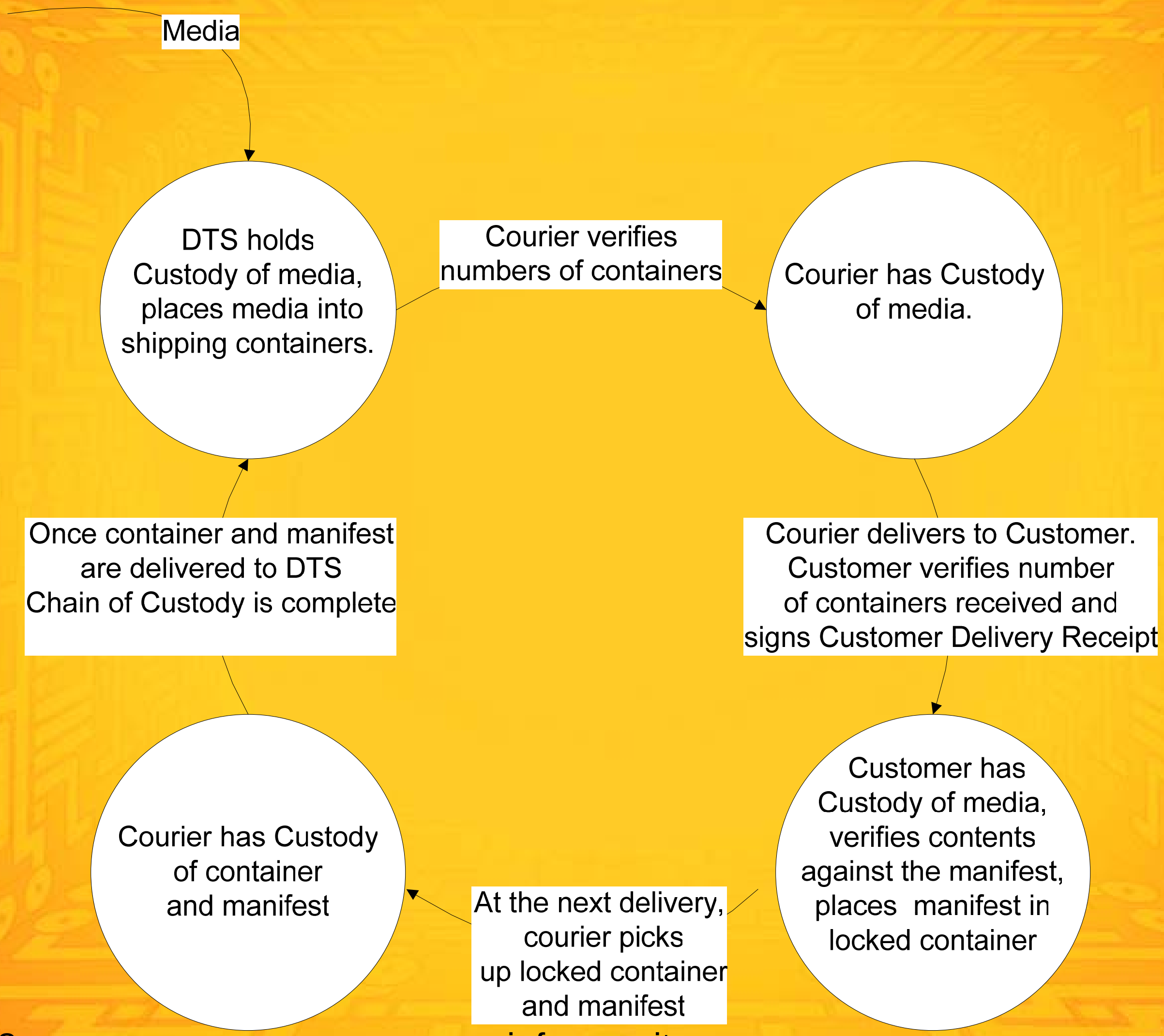
What is Chain of Custody?

- Act, manner, handling, supervision, and/or control of media or information.
- Preserve the integrity of the media resources.

What is DTS doing to protect your media?

- Verification
- Escalation
- Sorting
- Secured containers
- Customer Delivery Receipts
- Customer Procedures
- Documentation

Chain of Custody Flowchart



Media

DTS holds Custody of media, places media into shipping containers.

Courier verifies numbers of containers

Courier has Custody of media.

Courier delivers to Customer. Customer verifies number of containers received and signs Customer Delivery Receipt

Customer has Custody of media, verifies contents against the manifest, places manifest in locked container

At the next delivery, courier picks up locked container and manifest

Courier has Custody of container and manifest

Once container and manifest are delivered to DTS Chain of Custody is complete

Sending in Media

- Send media back to DTS in secured containers
- Download Customer Delivery Receipt and Job Handling Manifest at DTS' website

“What If…?”

- Missing media
- Discrepancy in the manifest
- Lost key
- Special courier run
- Lost or damaged container
- Missed delivery

Media Chain of Custody Analysis - Scope/Objectives

- Assess DTS' current IT operations media handling processes.
- Identify alternatives to address process improvements for secure handling and transmission of print, computer output microfilm (COM), magnetic tape, and the Chain of Custody system.
- Recommend process improvements and best practices associated with the secure handling and transfer of output media.
- Provide cost data to facilitate development of a Feasibility Study Report (FSR).

Print Recommendations

- Replace DTS customers print reports with an online viewing and archiving report management system.
- Online viewing is more secure, less expensive, easy to use (e.g., quick retrieval, search capability, individual security settings.)
- DTS already has successful experience.

COM Recommendations

- Replace DTS customers fiche with an online viewing and archiving report management system.
  - Eliminating fiche storage is more efficient and more secure.
  - Determine whether to convert archived fiche to disk on an individual customer basis.
- Online viewing is less expensive and easy and quicker to retrieve archived data.
  - DTS already has a successful experience of replacing fiche with online report viewing.
- Security enhancements would continue to final user, not just to DTS customer.

Tape Recommendations

- Eliminate tape delivery to increase security.
  - Eliminating tape transport is more secure.
  - As tape volume decreases tape handling costs will increase.
  - Change to electronic data transfer methods already used by some customers.
  - Convert COM tape jobs to online and use existing T1 lines.
- Customers have a choice of proven technologies.
  - Use secure FTP software.
  - Tumbleweed is easy to use.
  - DTS already has successful experience with all suggested secure file transfer technologies.

Chain of Custody Recommendations

- Phase out courier delivery to increase security.
  - Eliminating courier data transport is more secure.
- Use different solutions for different types of media.
- There is a high security risk and cost of using physical media to transport data-at-rest.
  - Secure electronic technology reduces risk of security breach.
- Use proven technology to help manage the transport of media.
  - Implement barcodes or RFID technology as interim increased security measure.
  - Secure electronic technology is less expensive.
  - DTS already has successful experience with all suggested technologies.

Now What?

- DTS will begin to market technologies to customers through Technology Days and other forums.
- DTS will take findings and recommendations to DTS Customer Council and Technology Services Board.

Thank You!

- Please complete your surveys.
- Look for future events here: http://www.dts.ca.gov/calendar/
- See you next time!